Approximate trapdoors for lattices & smaller hash-and-sign signatures

Yilei Chen — Visa Research

Nicholas Genise — UCSD -> Rutgers

Pratyay Mukherjee — Visa Research

Lattice signatures in NIST PQC (128-bit security)

Scheme	Assumption, feature	PK size	Signature size
Falcon	NTRU, trapdoor	0.9 kB	0.6 kB
Dilithium	MLWE, rejection sampling	1.5 kB	2.7 kB
q-Tesla	RingLWE, rejection sampling	4.1 kB	3.1 kB

Lattice signatures in NIST PQC (128-bit security)

Scheme	Assumption, feature	PK size	Signature size
Falcon	NTRU, trapdoor	0.9 kB	0.6 kB
Dilithium	MLWE, rejection sampling	1.5 kB	2.7 kB
q-Tesla	RingLWE, rejection sampling	4.1 kB	3.1 kB
GPV08+MP12	RingLWE, trapdoor	???	???

Lattice signatures in NIST PQC (128-bit security)

Scheme	Assumption, feature	PK size	Signature size
Falcon	NTRU, trapdoor	0.9 kB	0.6 kB
Dilithium	MLWE, rejection sampling	1.5 kB	2.7 kB
q-Tesla	RingLWE, rejection sampling	4.1 kB	3.1 kB
GPV08+MP12	RingLWE, trapdoor	35 kB*	25 kB*

*Relatively close to the textbook schemes, without heavy optimizations.

[BB13] Rachid El Bansarkhani and Johannes A. Buchmann.
Improvement and efficient implementation of a lattice-based signature scheme.
[GPRRS18] Kamil Doruk Gur, Yuriy Polyakov, Kurt Rohloff, Gerard W Ryan, and Erkay Savas.
Implementation and evaluation of improved gaussian sampling for lattice trapdoors.

Lattice signatures in NIST PQC (128-bit security)

Scheme	Assumption, feature	PK size	Signature size
Falcon	NTRU, trapdoor	0.9 kB	0.6 kB
Dilithium	MLWE, rejection sampling	1.5 kB	2.7 kB
q-Tesla	RingLWE, rejection sampling	4.1 kB	3.1 kB
GPV08+MP12	RingLWE, trapdoor	35 kB*	25 kB*
This work	RingLWE, approximate trapdoor	Smaller 😛	Smaller 😛

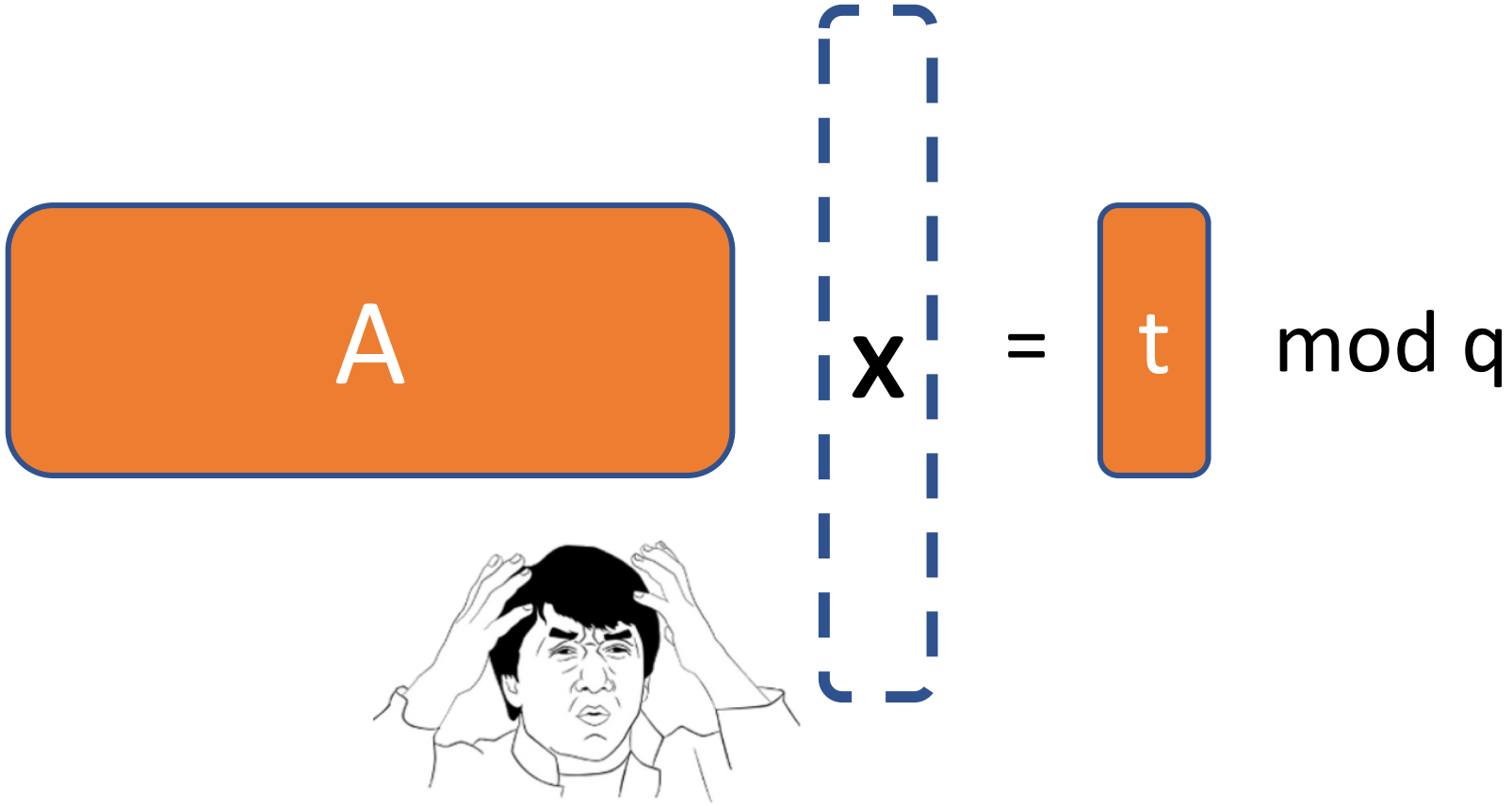
The rest of the talk:

1. Recall GPV signature with exact trapdoors.
2. Approximate trapdoor construction and analysis*.
3. Parameters.

Recall ISIS

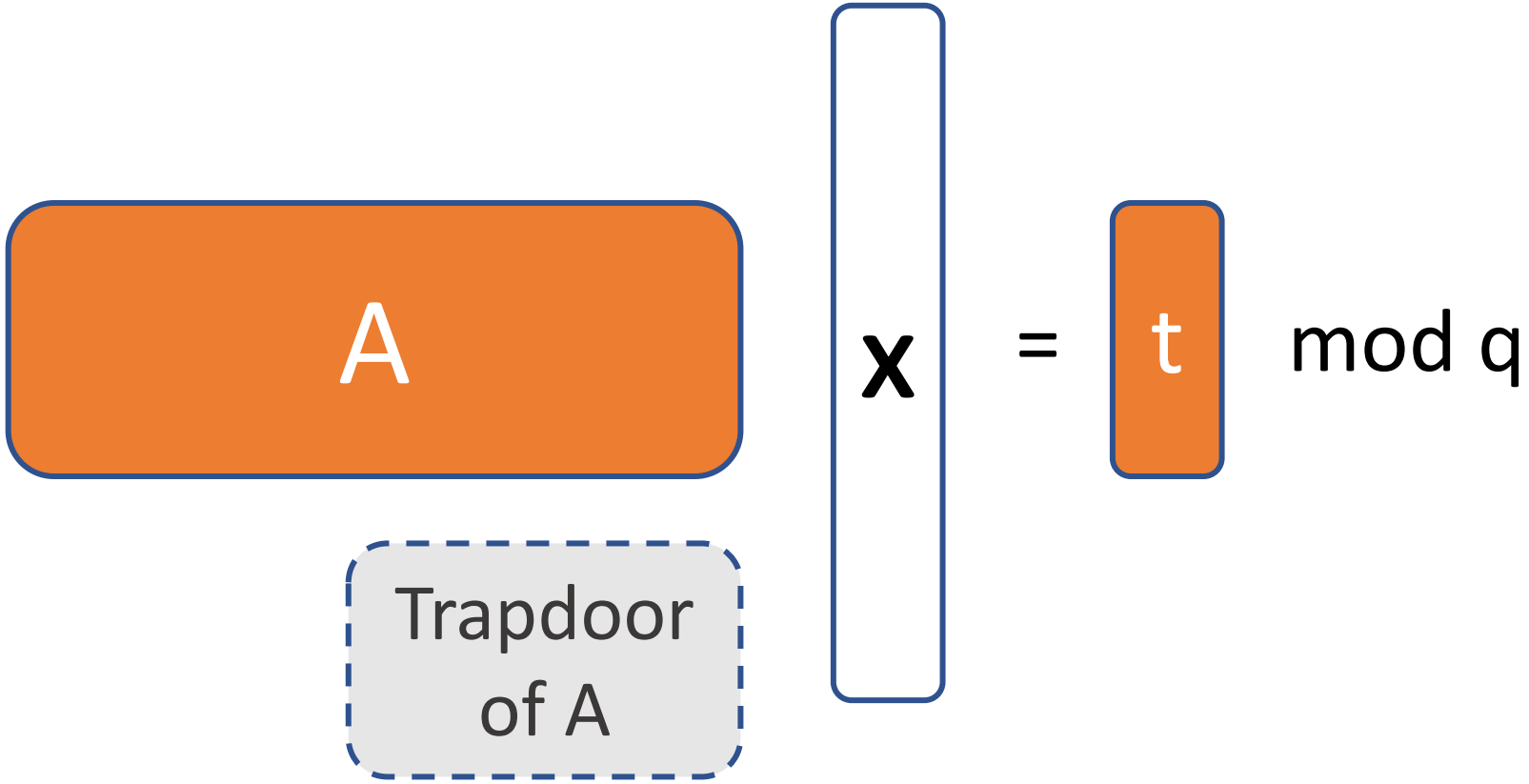
Inhomogeneous Short Integer Solution (ISIS):
Given A, t, find a short vector x.

Recall ISIS



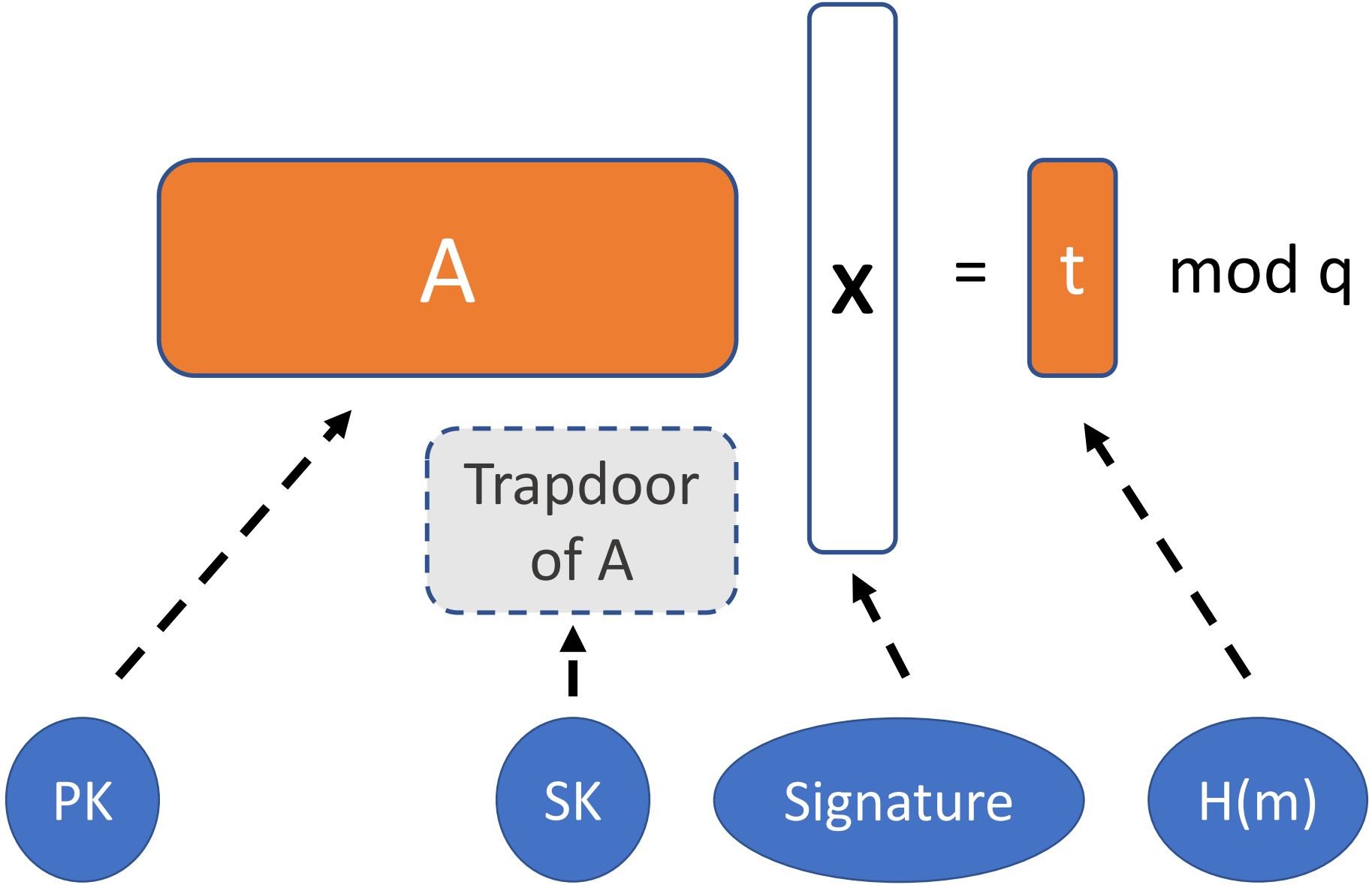
Inhomogeneous Short Integer Solution (ISIS):
Given A, t, find a short vector x.

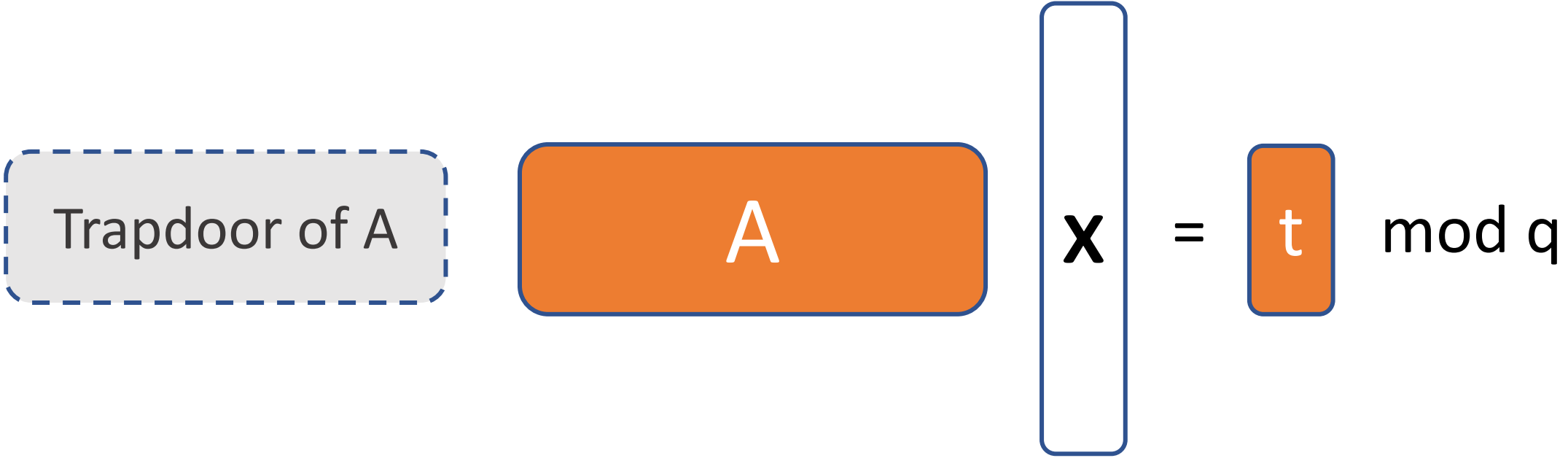
Recall Trapdoor

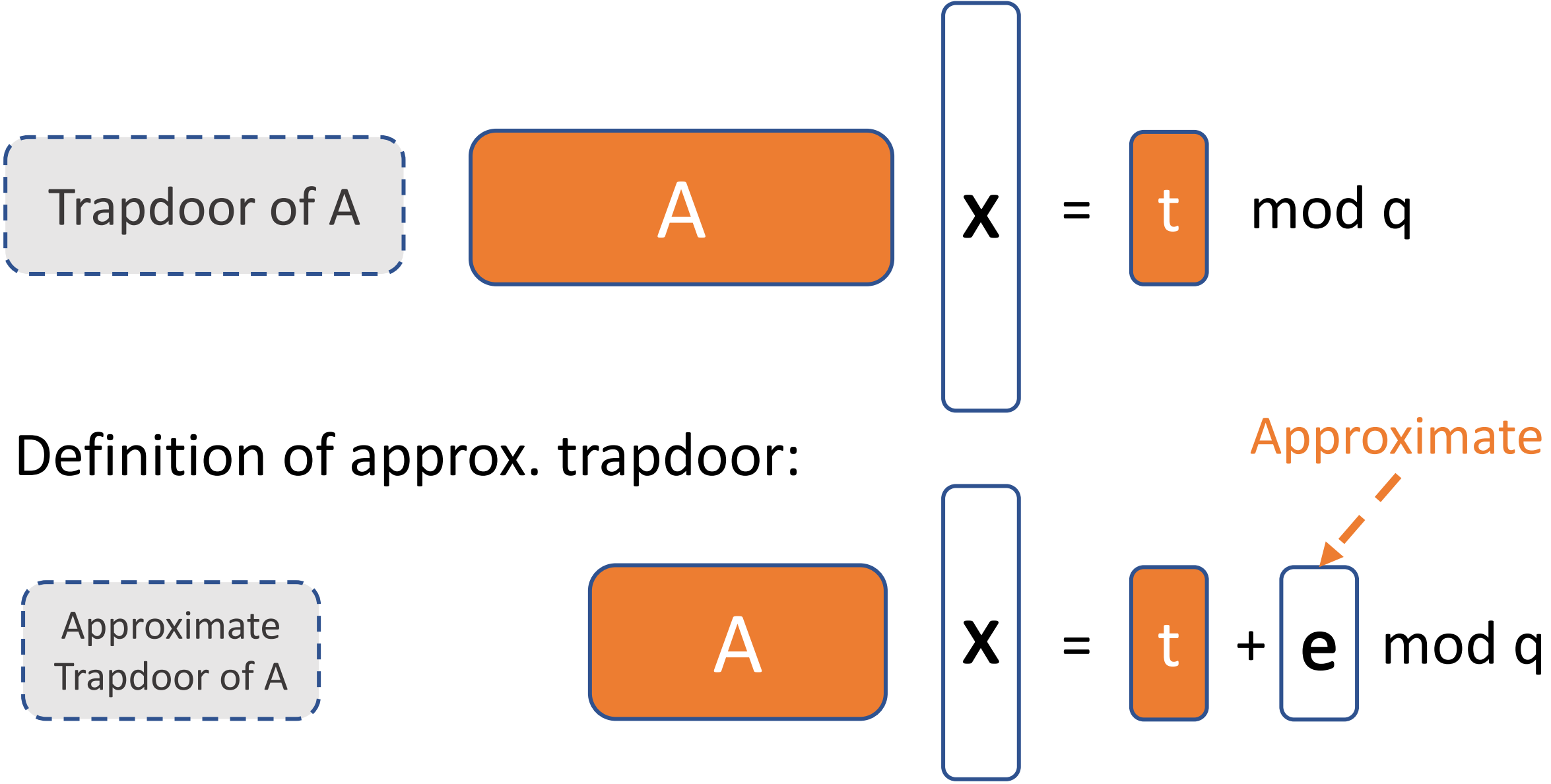


With the Trapdoor of A --> can solve ISIS efficiently.

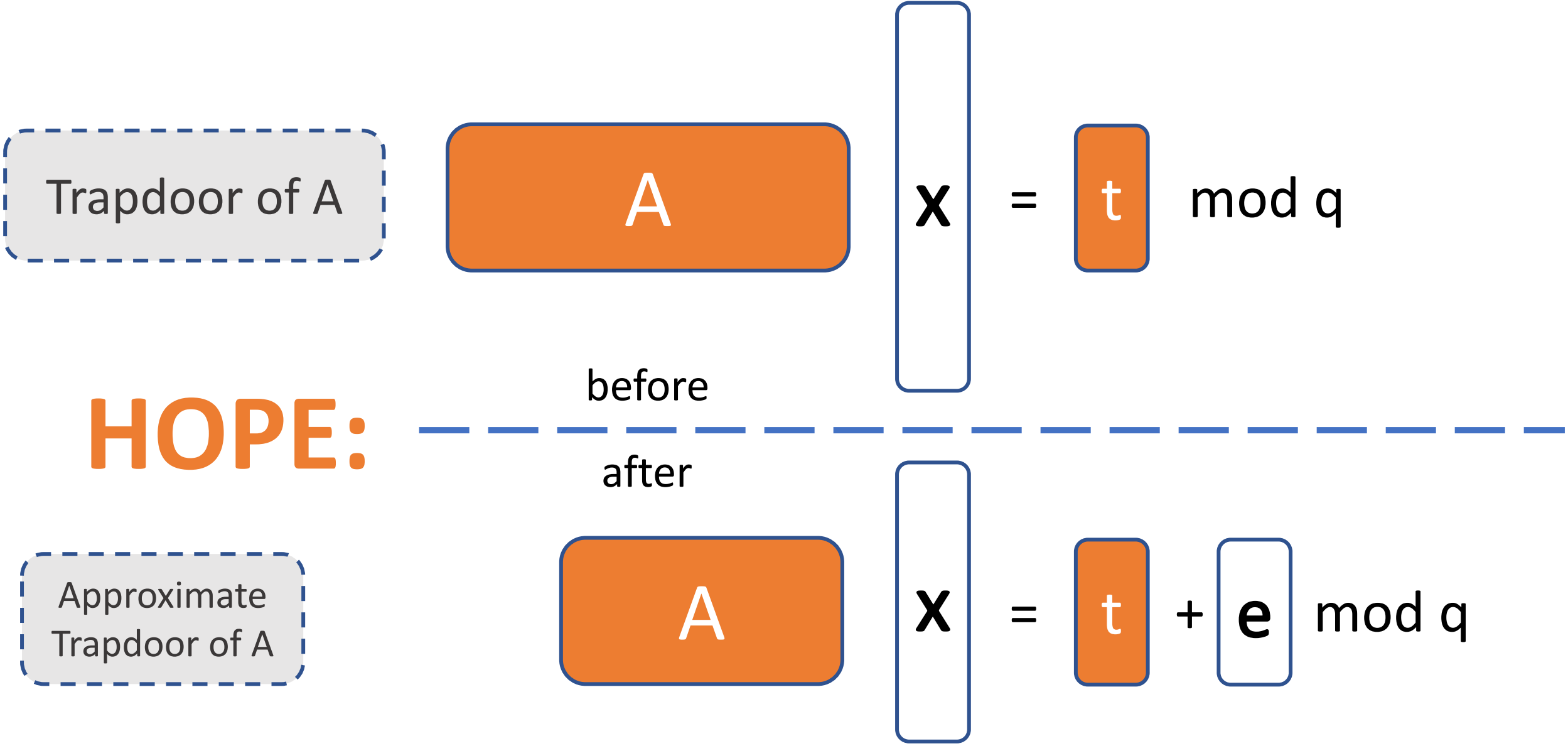
Recall GPV signature [Gentry, Peikert, Vaikuntanathan 08]




Trapdoor of A
A
x
=
t
mod q



Find a short x such that $Ax \approx t \; mod \; q$



Hope: an approximate trapdoor can be set up with a smaller dimension.

Trapdoor of A

$I_n \mid A'$

$\begin{matrix} x_1 \\ \vdots \\ x_2 \end{matrix}$ = t mod q

Solution 1:
Hermite Normal Form

before

Trapdoor of A

$I_n \mid A'$ $\begin{pmatrix} x_1 \\ --- \\ x_2 \end{pmatrix} = t \mod q$

Solution 1:
Hermite Normal Form

before

after

Approximate
Trapdoor of A'

A' $x_2 = t - x_1 \mod q$

Let $A \in Z^{n \times m}$. The HNF solution saves n dimensions.

Can we save more?

The rest of the talk:

~~1. Recall GPV signature with exact trapdoor.~~

2. Constructing approximate trapdoor.

3. Parameters.

Trapdoor from [Micciancio, Peikert 12]

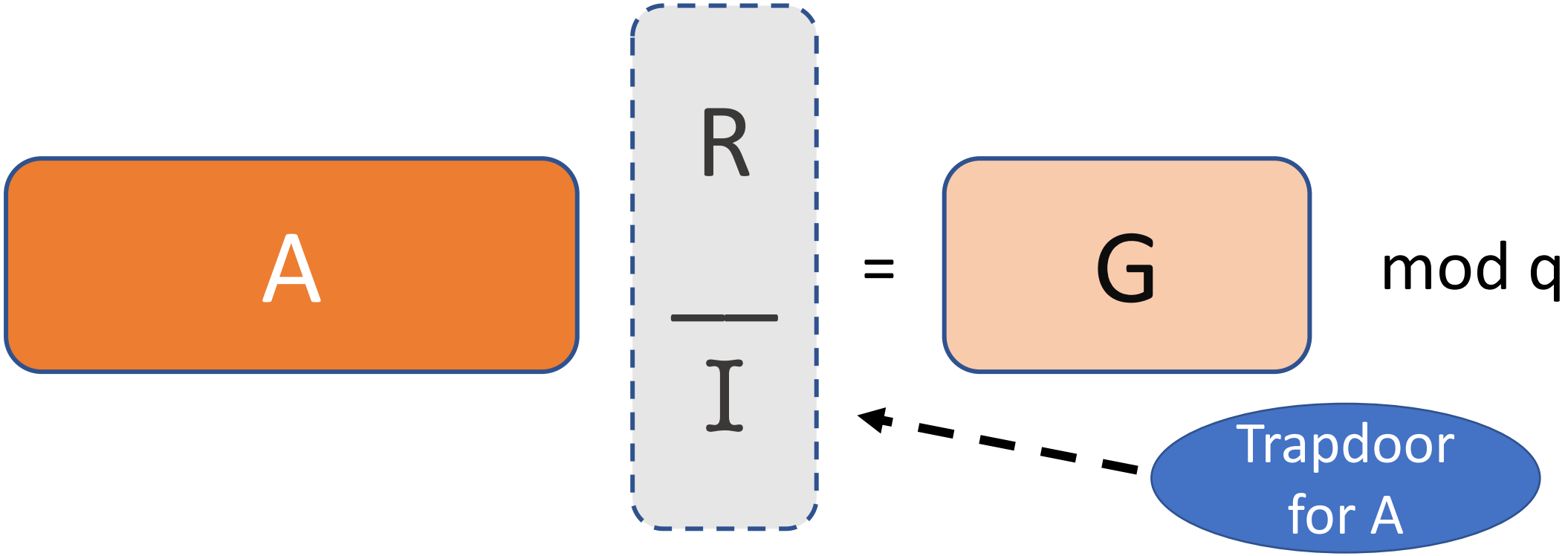
Let $k = \log_b q$. $G \in Z^{n \times nk}$

Gadget G = $\begin{matrix} 1, b, \ldots b^{k-1} \\ \ldots \ldots \\ 1, b, \ldots b^{k-1} \end{matrix}$ = $I_n \otimes$ (1, b, … b^{k-1})

"Power-of-b" matrix

The kernel-lattice of G has an easily computable short basis.

Trapdoor from [Micciancio, Peikert 12]



where A = [A' | G – A'R]

Let $k = \log_b q$. We have $G \in Z^{n \times nk}$, $A \in Z^{n \times n(2+k)}$

Gadget $\mathbf{G}$ = $\begin{matrix} 1, b, \dots b^{k-1} \\ \dots \dots \\ 1, b, \dots b^{k-1} \end{matrix}$ = $I_n \otimes$ $1, b, \dots b^{k-1}$

Core Idea

Approximate trapdoor

before

Gadget $G = \begin{matrix} 1, b, \dots b^{k-1} \\ \dots \dots \\ 1, b, \dots b^{k-1} \end{matrix} = I_n \otimes (1, b, \dots b^{k-1})$

Core Idea

Approximate trapdoor

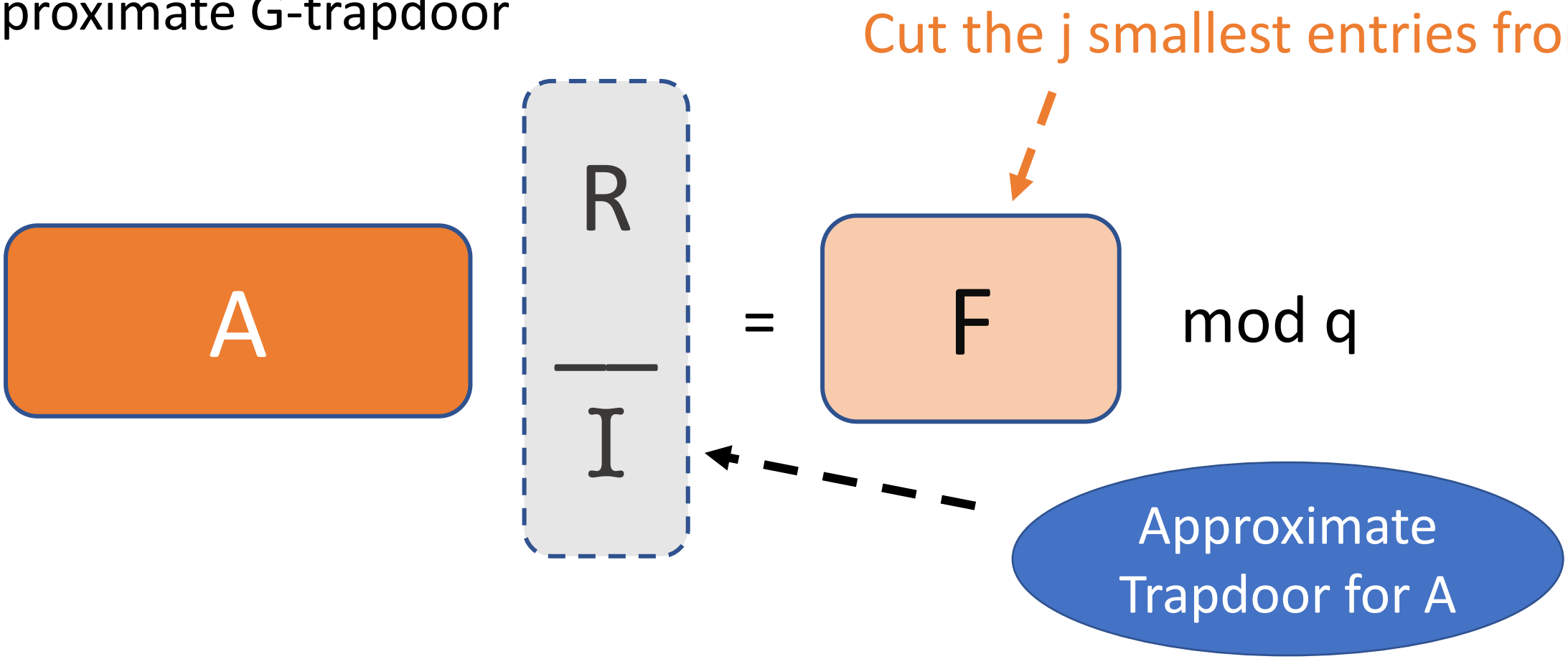
before

after

Smaller Gadget $F = \begin{matrix} b^j, \dots b^{k-1} \\ \dots \dots \\ b^j, \dots b^{k-1} \end{matrix} = I_n \otimes (b^j, \dots b^{k-1})$

Cut the j smallest entries from G

Approximate G-trapdoor



where A = [A' | F – A'R]

Let $k = \log_b q$. We have $F \in Z^{n \times n(k-j)}$, $A \in Z^{n \times n(2+k-j)}$

The preimage sampling algorithm

Input: A, the trapdoor R, a target $t \in Z^n$, a width parameter s.

Output: $x \in Z^m$ such that $Ax = t + e \; mod \; q$,

and x, e are from distributions independent of the trapdoor.

The preimage sampling algorithm

Input: A, the trapdoor R, a target $t \in Z^n$, a width parameter s.

Output: $x \in Z^m$ such that $Ax = t + e \; mod \; q$,

and x, e are from distributions independent of the trapdoor.

1. Sample a perturbation $p \leftarrow D_{\{Z^m, \sqrt{\Sigma_p}\}}$, where $\Sigma_p = sI_m - \sigma^2 \begin{bmatrix} RR^T & R \\ R^T & I \end{bmatrix}$

The preimage sampling algorithm

Input: A, the trapdoor R, a target $t \in Z^n$, a width parameter s.

Output: $x \in Z^m$ such that $Ax = t + e \; mod \; q$,

and x, e are from distributions independent of the trapdoor.

1. Sample a perturbation $p \leftarrow D_{\{Z^m, \sqrt{\Sigma_p}\}}$, where $\Sigma_p = sI_m - \sigma^2 \begin{bmatrix} RR^T & R \\ R^T & I \end{bmatrix}$
2. Form $v = t - Ap \in Z_q^n$.

The preimage sampling algorithm

Input: A, the trapdoor R, a target $t \in Z^n$, a width parameter s.

Output: $x \in Z^m$ such that $Ax = t + e \; mod \; q$,

and x, e are from distributions independent of the trapdoor.

1. Sample a perturbation $p \leftarrow D_{\{Z^m, \sqrt{\Sigma_p}\}}$, where $\Sigma_p = sI_m - \sigma^2 \begin{bmatrix} RR^T & R \\ R^T & I \end{bmatrix}$
2. Form $v = t - Ap \in Z_q^n$.
3. Sample y $\leftarrow D_{\{\Lambda_v^{\perp}(G), \sigma\}} \in Z^{nk}$, then drop the entries correspond to the j small entries in each block of size k. Denote the result as $z \in Z^{n(k-j)}$.

The preimage sampling algorithm

Input: A, the trapdoor R, a target $t \in Z^n$, a width parameter s.

Output: $x \in Z^m$ such that $Ax = t + e \; mod \; q$,

and x, e are from distributions independent of the trapdoor.

1. Sample a perturbation $p \leftarrow D_{\{Z^m, \sqrt{\Sigma_p}\}}$, where $\Sigma_p = sI_m - \sigma^2 \begin{bmatrix} RR^T & R \\ R^T & I \end{bmatrix}$
2. Form $v = t - Ap \in Z_q^n$.
3. Sample y $\leftarrow D_{\{\Lambda_v^{\perp}(G), \sigma\}} \in Z^{nk}$, then drop the entries correspond to the j small entries in each block of size k. Denote the result as $z \in Z^{n(k-j)}$.
4. Output $x = p + \begin{bmatrix} R \\ I \end{bmatrix} z$

The preimage sampling algorithm

Input: A, the trapdoor R, a target $t \in Z^n$, a width parameter s.

Output: $x \in Z^m$ such that $Ax = t + e \; mod \; q$,

and x, e are from distributions independent of the trapdoor.

1. Sample a perturbation $p \leftarrow D_{\{Z^m, \sqrt{\Sigma_p}\}}$, where $\Sigma_p = sI_m - \sigma^2 \begin{bmatrix} RR^T & R \\ R^T & I \end{bmatrix}$
2. Form $v = t - Ap \in Z_q^n$.
3. Sample y $\leftarrow D_{\{\Lambda_v^\perp(G), \sigma\}} \in Z^{nk}$, then drop the entries correspond to the j small entries in each block of size k. Denote the result as $z \in Z^{n(k-j)}$.
4. Output $x = p + \begin{bmatrix} R \\ I \end{bmatrix} z$

Small entries

dropped entries

Correctness: Write (a permuted version of) $G = [\, M \mid F \,]$, and $Gy = [\, M \mid F \,] \begin{bmatrix} n \\ z \end{bmatrix}$

The preimage sampling algorithm

Input: A, the trapdoor R, a target $t \in Z^n$, a width parameter s.

Output: $x \in Z^m$ such that $Ax = t + e \ mod \ q$,

and x, e are from distributions independent of the trapdoor.

1. Sample a perturbation $p \leftarrow D_{\{Z^m, \sqrt{\Sigma_p}\}}$, where $\Sigma_p = sI_m - \sigma^2 \begin{bmatrix} RR^T & R \\ R^T & I \end{bmatrix}$
2. Form $v = t - Ap \in Z_q^n$.
3. Sample y $\leftarrow D_{\{\Lambda_v^\perp(G), \sigma\}} \in Z^{nk}$, then drop the entries correspond to the j small entries in each block of size k. Denote the result as $z \in Z^{n(k-j)}$.
4. Output $x = p + \begin{bmatrix} R \\ I \end{bmatrix} z$

Small entries

dropped entries

Correctness: Write (a permuted version of) $G = [\ M \mid F\ ]$, and $Gy = [\ M \mid F\ ] \begin{bmatrix} n \\ z \end{bmatrix}$

So $Ax = Ap + A \begin{bmatrix} R \\ I \end{bmatrix} z = Ap + Fz = Ap + Gy - Mn = Ap + v + e = t + e$

Analysis of the distributions*

Notation: $G = [\, M \mid F \,]$, $Gy = [\, M \mid F \,] \begin{bmatrix} n \\ z \end{bmatrix}$, $\Sigma_p = sI_m - \sigma^2 \begin{bmatrix} RR^T & R \\ R^T & I \end{bmatrix}$

$$Ax = Ap + A \begin{bmatrix} R \\ I \end{bmatrix} z = Ap + Fz = Ap + Gy - Mn = Ap + v + e = t + e$$

Goal: x, e are from distributions independent of the trapdoor.

Analysis of the distributions*

Notation: $G = [\, M \mid F \,]$, $Gy = [\, M \mid F \,] \begin{bmatrix} n \\ z \end{bmatrix}$, $\Sigma_p = sI_m - \sigma^2 \begin{bmatrix} RR^T & R \\ R^T & I \end{bmatrix}$

$$Ax = Ap + A \begin{bmatrix} R \\ I \end{bmatrix} z = Ap + Fz = Ap + Gy - Mn = Ap + v + e = t + e$$

Goal: x, e are from distributions independent of the trapdoor.

Idea: first prove for all t, $(p, y) = (p, z, n) \leftarrow D_{\left\{\Lambda_t^{\perp}[\, A \,,\, G \,]\,, \sqrt{\Sigma_p \oplus \sigma^2}\right\}}$

Analysis of the distributions*

Notation: $G = [\, M \mid F \,],\ Gy = [\, M \mid F \,] \begin{bmatrix} n \\ z \end{bmatrix}, \Sigma_p = sI_m - \sigma^2 \begin{bmatrix} RR^T & R \\ R^T & I \end{bmatrix}$

$$Ax = Ap + A \begin{bmatrix} R \\ I \end{bmatrix} z = Ap + Fz = Ap + Gy - Mn = Ap + v + e = t + e$$

Goal: x, e are from distributions independent of the trapdoor.

Idea: first prove for all t, $(p, y) = (p, z, n) \leftarrow D_{\left\{\Lambda_t^{\perp}[\,A\,,\ G\,],\sqrt{\Sigma_p \oplus \sigma^2}\right\}}$

Next, derive (x, e) from (p, z, n) using linear transformation theorems on Gaussians.

I.e., consider two linear transformations L, M such that

$$L(p, z) = x, \qquad Mn = e$$

Analysis of the distributions*

Notation: $G = [\, M \mid F \,],\ Gy = [\, M \mid F \,] \begin{bmatrix} n \\ z \end{bmatrix}, \Sigma_p = sI_m - \sigma^2 \begin{bmatrix} RR^T & R \\ R^T & I \end{bmatrix}$

$$Ax = Ap + A \begin{bmatrix} R \\ I \end{bmatrix} z = Ap + Fz = Ap + Gy - Mn = Ap + v + e = t + e$$

Goal: x, e are from distributions independent of the trapdoor.

Idea: first prove for all t, $(p, y) = (p, z, n) \leftarrow D_{\left\{\Lambda_t^{\perp}[\, A\,,\ G\,],\sqrt{\Sigma_p \oplus \sigma^2}\right\}}$

Next, derive (x, e) from (p, z, n) using linear transformation theorems on Gaussians.

Theorem 2.7 ([Mic]). *For any positive definite Σ, vector $\mathbf{c}$, lattice coset $A := \Lambda + \mathbf{a} \subset \mathbf{c} + span(\Sigma)$, and linear transformation $\mathbf{T}$, if the lattice $\Lambda_{\mathbf{T}} = \Lambda \cap ker(\mathbf{T})$ satisfies $span(\Lambda_{\mathbf{T}}) = ker(\mathbf{T})$ and $\eta_\epsilon(\Lambda_{\mathbf{T}}) \leq \sqrt{\Sigma}$, then*

$$\mathbf{T}(D_{A,\mathbf{c},\sqrt{\Sigma}}) \overset{\bar{\epsilon}}{\approx} D_{\mathbf{T}A,\mathbf{T}\mathbf{c},\mathbf{T}\sqrt{\Sigma}}$$

where $\bar{\epsilon} = 2\epsilon/(1-\epsilon)$.

--- From personal communication with Micciancio.

Analysis of the distributions*

Notation: $G = [\, M \mid F \,],\ Gy = [\, M \mid F \,] \begin{bmatrix} n \\ z \end{bmatrix}, \Sigma_p = sI_m - \sigma^2 \begin{bmatrix} RR^T & R \\ R^T & I \end{bmatrix}$

$$Ax = Ap + A \begin{bmatrix} R \\ I \end{bmatrix} z = Ap + Fz = Ap + Gy - Mn = Ap + v + e = t + e$$

Goal: x, e are from distributions independent of the trapdoor.

Idea: first prove for all t, $(p, y) = (p, z, n) \leftarrow D_{\left\{\Lambda_t^{\perp}[\, A\,,\ G\,],\sqrt{\Sigma_p \oplus \sigma^2}\right\}}$

Next, derive (x, e) from (p, z, n) using linear transformation theorems on Gaussians.

Theorem 2.7 ([Mic]). *For any positive definite Σ, vector $\mathbf{c}$, lattice coset $A := \Lambda + \mathbf{a} \subset \mathbf{c} + span(\Sigma)$, and linear transformation $\mathbf{T}$, if the lattice $\Lambda_{\mathbf{T}} = \Lambda \cap ker(\mathbf{T})$ satisfies $span(\Lambda_{\mathbf{T}}) = ker(\mathbf{T})$ and $\eta_\epsilon(\Lambda_{\mathbf{T}}) \leq \sqrt{\Sigma}$, then*

$$\mathbf{T}(D_{A,\mathbf{c},\sqrt{\Sigma}}) \overset{\bar{\epsilon}}{\approx} D_{\mathbf{T}A,\mathbf{T}\mathbf{c},\mathbf{T}\sqrt{\Sigma}}$$

where $\bar{\epsilon} = 2\epsilon/(1-\epsilon)$.

(a special case proven by Ducas, Galbraith, Prest, Yu [eprint 2019/320] suffices for our app.)

Analysis of the distributions*

Notation: $G = [\, M \mid F \,]$, $Gy = [\, M \mid F \,] \begin{bmatrix} n \\ z \end{bmatrix}$, $\Sigma_p = sI_m - \sigma^2 \begin{bmatrix} RR^T & R \\ R^T & I \end{bmatrix}$

$$Ax = Ap + A \begin{bmatrix} R \\ I \end{bmatrix} z = Ap + Fz = Ap + Gy - Mn = Ap + v + e = t + e$$

Goal: x, e are from distributions independent of the trapdoor.

Idea: first prove for all t, $(p, y) = (p, z, n) \leftarrow D_{\left\{ \Lambda_t^{\perp}[\, A \,,\, G \,],\, \sqrt{\Sigma_p \oplus \sigma^2} \right\}}$

Next, derive (x, e) from (p, z, n) using linear transformation theorems on Gaussians.

Still, we are only able to show for uniformly random t (although it is enough for the signature application),

$$x \leftarrow D_{\{ Z^m,\, s \}}, \quad e \leftarrow D_{\left\{ Z^{nj},\ \sigma \sqrt{(b^{2j}-1)/(b^2-1)} \right\}}$$

Open problem: prove or disprove the statement for all t.

Parameters

	Exact	Approx	Exact	Approx	Exact	Approx	Exact	Approx
n	512		512		1024		1024	
$\log_2 q$	24		16		18		18	
b	2		4		4		8	
k/j	24/0		8/0		9/0		6/0	
|PK| (kB)	37.50		9.00		22.50		15.75	
|Sig| (kB)	25.68		7.62		18.74		13.70	
LWE	100.0		104.7		192.7		192.7	
ApproxISIS	80.2		82.8		175.8		165.3	

Parameters

	Exact	Approx	Exact	Approx	Exact	Approx	Exact	Approx
n	512	512	512	512	1024	1024	1024	1024
$\log_2 q$	24	24	16	16	18	18	18	18
b	2	2	4	4	4	4	8	8
k/j	24/0	24/15	8/0	8/4	9/0	9/5	6/0	6/3
|PK| (kB)	37.50	15.00	9.00	5.00	22.50	11.25	15.75	9.00
|Sig| (kB)	25.68	10.51	7.62	4.45	18.74	9.38	13.70	8.36
LWE	100.0	100.0	104.7	104.7	192.7	192.7	192.7	192.7
ApproxISIS	80.2	81.1	82.8	87.8	175.8	183.7	165.3	174.9

Approximate trapdoors for lattices & smaller hash-and-sign signatures

Q & A

Yilei Chen
Visa Research

Nicholas Genise
UCSD -> Rutgers

Pratyay Mukherjee
Visa Research